УДК 343.3/.7

Владислав Геннадійович КУНДЕУС,
кандидат юридичних наук, доцент,
доцент кафедри кримінально-правових дисциплін факультету № 6
Харківського національного університету внутрішніх справ

ПОНЯТТЯ ТА ВИДИ КІБЕРЗЛОЧИНІВ

Політика в сфері протидії кіберзлочинності здійснюється різноманітними засобами. Найбільш ефективними у системи її протидії залишаються засоби кримінально-правового впливу. Діяльність з протидії кіберзлочинам засобами кримінально-правового впливу ґрунтується на їх криміналізації. Хоча поняття «кіберзлочинність», «кіберзлочини» використовується як у міжнародному, так і у національному законодавстві, Кримінальний кодекс (далі – КК України) не містить визначення поняття кіберзлочину.

В кримінально-правовій та кримінологічній доктрині дискутуються різні точки зору щодо їх поняття, видів та класифікації. Законодавча невизначеність понять породила дискусійність питання про тлумачення, що є кіберзлочинами, та умовно поділила науковців на дві групи. Перша група науковців відносить до кіберзлочинів дії, у яких комп'ютер є об'єктом або засобом посягання. Друга група визначає кіберзлочини як злочини, об'єктом посягання в яких є інформація, що обробляється в електронно-обчислювальній машині (комп'ютері) або в комп'ютерній системі, а засобом вчинення є електронно-обчислювальна машина (комп'ютер), тобто протизаконні дії у сфері автоматичної обробки інформації [1, с. 7]. Але, в цілому, до таких злочинів відносять злочини, що вчиняються з використанням електронно-обчислювальних машин (комп'ютерів) та комп'ютерних мереж. До основних видів цих злочинів відносять: створення та поширення шкідливих програмних чи технічних засобів (вірусів), втручання у роботу комп'ютерів, автоматизованих систем та комп'ютерних мереж, крадіжку інформації, поширення протиправної інформації через систему Інтернет, фішинг, фармінг тощо.

У міжнародній доктрині поняттями кіберзлочини, кіберзлочинність охоплюються різні види правопорушень. У п. 14 Доповіді Комітету II Десятого Конгресу ООН 2000 року по попередженню злочинності і поводженню з правопорушниками було зазначено, що існує дві категорії кіберзлочинів: 1) кіберзлочини у вузькому розумінні («комп'ютерні злочини»): будь-яке протиправне діяння, здійснюване шляхом електронних операцій, метою якого є подолання захисту комп'ютерних систем і оброблюваних ними даних; 2) кіберзлочини в широкому розумінні («злочини, пов'язані з використанням комп'ютерів»): будь-яке протиправне діяння, яке вчиняється шляхом або в зв'язку з комп'ютерною системою або мережею, включаючи такі злочини, як незаконне зберігання, пропонування або розповсюдження інформації через комп'ютерні системи або мережі [2, с. 434–435].

Найбільш поширена класифікація кіберзлочинів в даний час ґрунтується на структурі Конвенції Ради Європи про кіберзлочинність від 23.11.2001 року. За конвенцією Ради Європи про кіберзлочинність існує чотири основних групи кіберзлочинів. До першої групи належать правопорушення проти конфіденційності, цілісності та доступності комп'ютерних даних і систем: незаконний доступ (ст. 2), нелегальне перехоплення (ст. 3), втручання у дані (ст. 4) втручання у систему (ст. 5), зловживання пристроями (ст. 6). До другої групи входять правопорушення, пов'язані з комп'ютерами: підробка та шахрайство, пов'язані з комп'ютерами (статті 7, 8). Третю групу складають правопорушення, пов'язані зі змістом: правопорушення, пов'язані з дитячою порнографією (ст. 9). До четвертої групи увійшли правопорушення, пов'язані з порушенням авторських та суміжних прав (ст. 10) [3].

Стратегія національної безпеки, затверджена Указом Президента України від 8 червня 2012 року № 389/2012, містить терміни «кіберзлочинність», «кіберзагроза», «кібербезпека» [4]. Згідно п.9 ст. 1 Закону України від 05.10.2017 року «Про основні засади забезпечення кібербезпеки України» кіберзлочинність – це сукупність кіберзлочинів. Кіберзлочин (комп'ютерний злочин) – це суспільно небезпечне винне діяння у кіберпросторі та/або з його використанням, відповідальність за яке передбачена законом України про кримінальну відповідальність та/або яке визнано злочином міжнародними договорами України (п. 8 ст. 1 Закону) [5]. Ґрунтуючись на цьому понятті, до кіберзлочинів (комп'ютерних злочинів) слід

відносити передбачені КК України суспільно небезпечні винні діяння, вчинені у кіберпросторі та/або з його використанням. Залежно від об'єкту посягання кіберзлочини (комп'ютерні злочини) можна класифікувати за такими видами:

1) Злочини, вчинені у кіберпросторі та/або з його використанням, відповідальність за які передбачена різними розділами КК України. Такі злочини посягають на різні об'єкти кримінально-правової охорони: основи національної безпеки, громадську безпеку, відносини у сфері охорони права на об'єкти інтелектуальної власності, власність, господарські відносини, права та свободи тощо. Ознакою віднесення цих злочинів до кіберзлочинів є те, що вони вчиняються з використанням сучасних інформаційних технологій і засобів комп'ютерної техніки. Наприклад: викрадення реквізитів платіжних карток (фішинг, вішинг, шиммінг, скимінг); незаконні фінансові операції з використанням платіжних карток або їх реквізитів, які не ініційовані або не підтверджені її власником (кардінг); заволодіння коштами через фіктивні інтернет-магазини, інтернет-аукціони, сайти та інші засоби телекомунікації (онлайн–шахрайство); порушення авторського права і суміжних прав шляхом незаконного розповсюдження програмних продуктів через комп'ютерні мережі (піратство) тощо.

2) Злочини у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж, що передбачені Розділом XVI КК України. Ознакою віднесення цих злочинів до комп'ютерних є те, що вони посягають на відносини, що виникають у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку.

Слід зазначити, що аналіз національного та міжнародного законодавства, з протидії кіберзлочинам, дозволяє стверджувати, що Україна вживає необхідних заходів, спрямованих на їх профілактику та протидію кримінально-правовими засобами. Проте, діяльність з протидії кіберзлочинам, насамперед, обмежена їх виключним переліком, що міститься у Кримінальному кодексі. Розділ VI Особливої частини «Злочини у сфері використання електронно-обчислювальних машин (комп'ютерів), систем і комп'ютерних мереж» передбачає відповідальність за окремі види кіберзлочинів, але їх перелік не повною мірою узгоджуються з класифікацією кіберзлочинів, передбаченою Конвенцією Ради Європи про кіберзлочинність. Криміналізація суспільно небезпечних діянь, вчинених у кіберпросторі, з урахуванням міжнародних документів буде сприяти вирішенню проблем законодавчого забезпечення протидії кіберзлочинності в Україні.

Список бібліографічних посилань

1. Амелін О. Визначення кіберзлочинів у національному законодавстві. *Науковий часопис Національної академії прокуратури України*. 2016. № 3. С. 1–10

2. Юртаєва К. В. Визначення місця вчинення злочинів з використанням комп'ютерних технологій. *Форум права*. 2009. № 2. С. 434–441. URL: http://nbuv.gov.ua/j-pdf/FP_index.htm_2009_2_69.pdf (дата звернення: 02.03.2020).

3. Конвенція про кіберзлочинність : від 23.11.2001 // База даних (БД) «Законодавство України» / Верховна Рада (ВР) України. URL: https://zakon.rada.gov.ua/laws/show/994_575/ (дата звернення: 02.03.2020).

4. Про рішення Ради національної безпеки і оборони України від 27 січня 2016 року «Про Стратегію кібербезпеки України» : Указ Президента України від 15.03.2016 № 96/2016 // БД «Законодавство України»/ ВР України. URL: https://zakon.rada.gov.ua/laws/show/96/2016 (дата звернення: 02.03.2020).

5. Про основні засади забезпечення кібербезпеки України : Закон України від 05.10.2017 № 2163-VIII // БД «Законодавство України» / ВР України. URL: https://zakon.rada.gov.ua/laws/show/2163-19 (дата звернення: 02.03.2020).

Одержано 05.03.2020